Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Information Management and Technology (IM&T) Security Policy

This procedural document supersedes: CORP/ICT 2 v.4 – Information Management and Technology (IM&T) Security Policy

Did you print this document yourself?

The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, it is only valid for 24 hours.**

Executive Sponsor(s):	Simon Marsh, CIO and SIRO
Author/reviewer: (this version)	Roy Underwood Robin Smith
Date written/revised:	October 2017 - June 2018
Approved by:	IG Group
Date of approval:	24 July 2018
Date issued:	13 September 2018
Next review date:	February 2021
Target audience:	Trust-wide

Amendment Form

Please record brief details of the changes made alongside the next version number. If the procedural document has been reviewed **without change**, this information will still need to be recorded although the version number will remain the same.

Version	Date Issued	Brief Summary of Changes	Author
Version 5	13 September 2018	• Revise to ensure compliance with GDPR and the Data Protection Act 2018 • To reflect the changes detailed in current versions of the Data Security & Protection (DSP) Toolkit from April 2018 (formerly the IG Toolkit), especially with regards to Cyber Security • Revision of policy statements to include wider range of subjects following external review by KPMG • Link to new procedural guidance in support of revised policy statements • Update of management responsibilities to include new IT Security Manager position	Robin Smith Roy Underwood
Version 4	22 October 2013	• Change to Policy Title and Layout (iaw CORP/COMM 1 Mask) • Updated network control policy. • Appendix B - Systems Implementation. All new processes, services, information systems, and other relevant information assets will be developed and implemented in a secure and structured manner.	Roy Underwood, Nigel Hall
Version 3	June 2009	• Complete re-write of the policy to reflect the changes detailed in version 7 of the IG Toolkit (July 2009), and in the NHS CEO's Gateway reference letter: 10509 dated September 2008. • All breaches of information security & confidentiality will be reported and investigated through the Trust's DATIX incident reporting system – Page 9. • Details of the responsibilities of the Trust Caldicott Guardian/Senior Information Risk Owner (SIRO) – Page 9. • Details of the responsibilities of the: - Information Security Officer (ISO) - CSU Managers and their Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) • Detailed responsibility for core information systems and their relevant systems managers – Page 11. • Reference to CORP/ICT 20 – Bulk Data Transfer	Roy G Underwood, Mark Norwood

		Policy • Appendix A: System Specific Security Arrangements with reference to IGT SoC Standard 305 and CORP/ICT 14 – Information Management (Code of Practice) – Page 29. • Remote working protocol	
Version 2	February 2007	Bi-annual review, incorporating amendments for: • The enforced User 'time-out' following a sustained period of User inactivity (DPA1998: Principle 7) – pages 12/13 • Risk Management Workshops – page 16 • USB Storage Device usage – page 22 • Unauthorized access to PC and VDU terminals – page 27	Roy G Underwood

Contents

Page No.

1 INTRODUCTION

The Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust ('the Trust') manages a great deal of personal and confidential data relating to patients, the public and employees of the NHS. It also creates information and records across its services on a daily basis, generating new knowledge about the organisation every day. These information assets are managed by a diverse array of digital information systems and are subject to a range of risks and threats.

The Trust recognises that information is the lifeblood of the Trust and its effective management has a significant impact on the delivery of all our services. Information assets must be protected from unauthorised use, disclosure, modification, damage and loss. Additionally, information assets must be available when needed, particularly during emergencies and times of high demand.

With emerging risks including cyber security and 'insider' threats it is essential that the Trust enhances its IM&T security standards. This will ensure that Trust digital information systems continue to maintain security standards and prevent potential problems occurring. The Trust requires a robust IM&T Security Policy and supporting procedures to manage and enforce standards to meet best practice requirements.

2 PURPOSE

The purpose of the policy is to safeguard the Trust's and patients' information within a secure digital environment. The IM&T Security policy will ensure that digital information systems protect all Trust data and information, limiting the risk of unauthorised access and promoting staff awareness of the value of information security management.

It is the policy of the Trust to ensure that:

- Information will be protected and controlled against unauthorised access.
- Confidentiality of information will be assured.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.

This top-level IT Security policy should be considered as a key component of the organisation's overall security management framework and should be considered alongside more detailed IT security documentation. For more information please see Appendix One of this policy document.

3 DUTIES AND RESPONSIBILITIES

The Chief Executive has overall responsibility for IM&T Security within the Trust. This responsibility is delegated to the Chief Information Officer (CIO) as Senior Information Risk Owner (SIRO), and to the Trust Caldicott Guardian. The latter officer has responsibility to the Information Governance Group and the Audit & Non Clinical Risk Assurance Committee (ANCR) on behalf of the Board of Directors for Trust compliance with the security standards set by national bodies including NHS Digital.

Ongoing monitoring of the policy and information security issues is the responsibility of the Information Governance Group (IG Group). The IG Group is responsible for monitoring and reviewing information security threats and incidents and plays a role in reviewing any initiatives for improving information security. The work of the IG Group is reviewed by the Integrated Governance Committee as part of the overall Risk Management Strategy.

The Caldicott Guardian and the SIRO have responsibility for placing appropriate controls and procedures in place for the monitoring of all information systems containing patient identifiable information created by Trust.

Operational management and implementation of this policy will be delegated to the IT Security Manager and the Head of Information Governance. These roles will collaborate to ensure that the requirements of this policy are developed, implemented and reviewed as part of an ongoing programme.

All Care Group & Departmental/Business Unit managers should:

- be aware of their IM&T security responsibilities as detailed in the policy including procedures for staff access levels to key systems and the need to provision access appropriately.
- ensure staff are aware of their IM&T Security responsibilities as detailed in this policy and that staff using digital information systems are trained in their use.
- investigate any IM&T security issues raised by members of staff in accordance with the Trust's Risk Management Policy (if applicable).
- address any IM&T security issues with the support of the Head of Information Governance and IT Security Manager.

All employees should:

- ensure that they comply with the requirements of the policy and related security procedures.
- report any observed or suspected security weaknesses or threats to systems or services to line managers or the Trust's IT Service Desk who will liaise with the appropriate members of staff.

A breach of the policy or any of the Acts described within may result in disciplinary proceedings.

4 PROCEDURE

4.1 IM&T Security Management Requirements

The following section contains all relevant security management requirements to promote better standards across services.

4.2 Management Security Requirements

Management should implement procedures to minimise the Trust's exposure to fraud/theft/disruption of information held within digital information systems. This would include designing access controls that promote segregation of duties and staff rotation in critical areas to avoid the risk arising of unauthorised access.

Management should determine which individuals are to be given authority to access specific digital information systems. The level of access to specific systems should be on a job function need, independent of status.

Management should also ensure that no unauthorised staff are allowed to access any of the Trust's digital information systems as such access could compromise data integrity.

4.3 Employee Security Requirements

All staff within the Trust are responsible for ensuring that any Trust information which they hold is securely managed and protected.

The Trust operates a clear screen policy that means users must ensure that workstations are locked or logged off if a workstation is left unattended. Users failing to comply may be subject to disciplinary action.

Staff have a responsibility to report any observed or suspected inappropriate accessing of sensitive Trust information to their line manager (see Whistle Blowing Policy for further options). Staff should themselves refrain from accessing information when they have no real 'need to know'.

Theft is a disciplinary offence. Staff should not make it easy for equipment to be stolen or vandalised e.g. making sure PCs are secure in unoccupied public areas.

4.4 Information Classification and Storage

Government Security Classification; Information should be managed carefully and if necessary classified in line with the Government Security Classification scheme.

All organisational files should be saved to the Trust network, which should be kept safe from fire, theft, flood and physical damage. Personal data should not be stored on the local hard drives or on any of the Trust's encrypted mobile storage devices without expressed knowledge and authority from a Trust senior manager.

For further information please see the Trust's procedure for Information and Data Classification, issued by the IT Security team.

4.5 Infrastructure Access Controls

Physical Access Controls; Entry to secure areas housing critical or sensitive infrastructure equipment will be restricted to those whose role requires it. The IT Security Manager will maintain and periodically review a list of those with unsupervised access.

All network devices will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.

Critical or sensitive network rooms will be protected by a secure perimeter, with appropriate security barriers and access controls.

The IT Security Manager is responsible for ensuring that door lock codes are changed periodically, following a compromise of the code, if s/he suspects the code has been compromised.

Critical or sensitive network equipment will be protected from power supply failures. Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.

Smoking, eating and drinking is not permitted in areas housing critical or sensitive network equipment.

Technical Access Controls; There must be a formal, documented user registration and de-registration procedure for access to the network or Trust digital information systems. Departmental managers must approve user access. Access rights to the network will be allocated on the requirements of the user's role.

Security privileges (i.e. 'super-user' or network administrator rights) to the network will be allocated on the requirements of the user's role and subject to audit by IT Security to ensure provisioning is in line with this policy.

Third Party Access Control; Third party access to the network will be based on a formal contract that satisfies all necessary NHS security conditions. All third party access to the Trust's network and digital information systems must be auditable.

External Network Connections; The Head of IT Operations is responsible for ensuring that all connections to external networks and systems conform to the NHS-wide Network Security Policy, Code of Connection and supporting guidance. The Head of IT Operations must approve all connections to external networks and systems before they commence operation.

Fault Logging; The IT Security Manager is responsible for ensuring that a log of all faults on the network is maintained and reviewed. A report of any faults and review of countermeasures will be taken to an IM&T service review group.

Data Backup and Restoration; The Head of IT Operations is responsible for ensuring that backup copies of network configuration, network storage and server data are taken regularly. All backup tapes will be stored securely in the secure safes.

Multi-Factor Authentication; Where possible the Trust will seek to implement multi-factor authentication to ensure access to Trust information and systems is controlled. Multi-factor authentication will include the use of access controls that are regularly audited for security.

Cryptographic Management Controls; Public key cryptography is a key part of the IT infrastructure and needs to be managed and maintained to the highest levels. The Trust regularly uses cryptographic methods to protect processes, including those for information sharing and for accessing external websites.

IT Security will ensure that cryptographic controls ultimately strengthen protective measures already defined for the protection of Trust information by implementing approved encryption methods. This will allow the Trust to manage its information with confidence and in line with all stated national best practice requirements.

4.6 Systems Acquisition, Development and Testing

Procuring New Systems; The procurement of new digital information systems and hardware should always be discussed with the Trust's IM&T senior management team, irrespective of the source of the funding. The IM&T Department will advise on the purchase of standardised and compatible systems and equipment, support and maintenance, and IT security issues.

Prior to acceptance, new systems shall be checked for technical compliance with the Trust's information security policies and standards.

Vulnerability Assessment and Penetration Testing; All Trust digital information systems should be regularly checked for technical vulnerabilities and / or penetration tested prior to entering live service, and during the operational lifecycle in accordance with the Trust's Vulnerability Management Policy.

Testing New Systems; The extent of any system testing shall be determined by the perceived threats and level of risk to which the system will be exposed and any specific

requirements from the NHS's regulatory framework. As a minimum, it is recommended a vulnerability scan is conducted to provide assurance that the system has been configured in a secure manner.

Testing facilities will be used for all new digital information systems and infrastructure. Development and operational facilities will be separated.

System Documentation; The IM&T Team leaders are responsible for updating all relevant design documentation, security operating procedures and computer network operating procedures appertaining to their specialty.

Securing Trust Systems; All Trust systems must establish baseline security requirements and be subject to testing throughout its lifetime. Security baselines are essential to meeting the demands of internal and external audit and provide business continuity in the event of service disruption.

The essential nature of a number of IM&T services including email, Internet and network access means that these systems need to be secured to the highest levels. Acceptable usage policies link to this document to ensure that systems are used for appropriate purposes.

4.7 Protective Monitoring

Securing External and Internal Boundaries; Protective monitoring is a key requirement of the IT Security Policy Framework and an essential component of risk treatment when accrediting Trust networks and services processing protectively marked information to national best practice standards.

The Trust will implement protective monitoring to set minimum standards for security incident and event management and data loss prevention.

Data Loss Prevention; It is essential that the Trust actively implements standards to prevent data loss via internal or external sources. This will include creating specific standards and audits to monitor threats to data loss and educating employees regarding the need for vigilance when dealing with sensitive information.

Security Incident and Event Monitoring (SIEM);SIEM supports Protective Monitoring by aggregating threat intelligence sources into management reports that can support decision making. Many different sources produce security incident information that can aid decision making in the event of security threats or incidents. Sources of intelligence include network servers, firewall logs and network clients.

The Trust will seek to actively monitor security incident data to produce threat intelligence reports, linking to external sources of data including updates from NHS Digital via CareCert.

Malware and Anti-Virus; IM&T will provide virus protection software for all Trust devices and monitor any required improvements in the effective operation of this key control. All

computers connected to the Trust's network must run an approved, licensed and up-to-date anti-virus product that continually monitors for malicious software.

Any third party owned devices that connect to the Trust network must be equipped with an appropriate anti-virus product or related end-point defence controls. The Trust reserves the right to disconnect any device or information system from the network if an infection is found or suspected. The asset will remain disconnected until the infection is removed.

4.8 Communications Security

Communications security is the means by which Trust information is passed in an intelligible form whilst still delivering content to intended recipients. The purpose of Communications security (COMSEC) is to ensure the security of telecommunications confidentiality and integrity of Trust Information.

This policy is designed to minimise the potential exposure to the Trust's network from damages which may result from unauthorised access to or use of organisational information assets. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, etc.

The Trust currently deploys various technical and procedural methods of ensuring the best possible COMSEC measures are in place to protect its or other interested parties' information in line with current NHS Digital guidance.

4.9 'Insider' Threat Monitoring

There have been instances where malicious behaviour by Trust employees has resulted in security incidents. To protect against future incidents the Trust will conduct internal monitoring in line with legislation and stated best practice to ensure that the threat from 'Insiders', employees who are deliberately seeking to inappropriately access Trust data, is remediated.

This will include regular communications to Trust employees regarding individual responsibilities and the need to report any unusual behaviour with regard to information access.

4.10 Change and Configuration Management

Change Management; IT security is reliant on an excellent approach to both change and configuration management across services. Organisational change is driven by the business needs of the Trust.

Change can be triggered either by the external environment or by an internal review of IM&T service requirements. The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to IT Services.

The purpose and objective of the Change Management process is to control the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to Trust services. Processes will be updated to ensure that change management is an effective part of IM&T services.

Configuration Management; Configuration management (CM) is a systems process for establishing and maintaining consistency of an IT product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.

The Trust must seek to maintain accurate records of the configuration of its IT products to ensure that in the event of disruption or loss of services that the product can be properly restored. This would include infrastructure, applications and other key services. Processes will be introduced to ensure that CM is implemented effectively.

Technical Vulnerability Management; Failure to maintain digital information systems or networks in a secure manner can leave them vulnerable to attack. Technical vulnerabilities discovered in software, typically announced on a daily basis, may be exploited by attackers to gain unauthorised access to computer systems and networks.

Often when vulnerabilities are discovered, the manufacturer or vendor will release a patch or other workaround in order to:

- Correct or mitigate against the vulnerability;
- Fix faults in the system or application code;
- Increase or alter functionality;
- Change or modify the software to make it less susceptible to accidental or malicious exploitation.

To minimise the risk and reduce the vulnerability being exploited, the Trust must monitor patches released by manufacturers and decide when and where deployment is appropriate as part of the Change Management process.

4.11 Asset Management

Managing Trust Assets; Trust systems are essential information assets and should be managed as such via a central management system. All IT assets should be identified and managed across its life cycle to comply with best practices for service delivery.

Disposal of Equipment and Re-use; Disposal of assets can only be authorised by a nominated senior officer including the Head of IT Operations, however disposal should be done with the relevant of IT Security Operating Procedures (Syop).

It should be ensured that data storage devices are purged of confidential data before disposal and securely destroyed. The procedures for disposal must be documented.

4.12 Security Incident Management

Monitoring for Events and Incidents; Security incident response processes are necessary to deal with an incident wherever and whenever it occurs.

This policy proposes a framework for producing security incident response plans, including:

- Identifying potential threats that may instigate a security incident;
- Planning responses to incidents, e.g. roles and responsibilities, communications etc;
- Reporting the occurrence and necessary escalations;
- Immediate initial response and supporting actions;
- Narrative – recording events occurring during the incident;
- Recovery measures, if required, to return to business as usual;
- Analysis of how the incident occurred, decisions taken whilst managing the incident and confirming the response plan was followed;
- Final report, including incident narrative, reasons for deviating from the incident response plan if appropriate, analysis of the incident and lessons learned;
- Recommendations to avert recurrences and improve security should also be included in the final report;

Any IM&T incident must be reported using the procedure in the Incident Reporting Policy and in the Information Governance Risk Management Policy.

4.13 Business Continuity Management

Providing Disaster Recovery; It is essential for the Trust to maintain its services with minimum disruption. The Trust's services, strategies and decisions are dependent on the continuity of service and our BCM must be structured to ensure the maximum availability of all key service provisions within the organisational infrastructure.

Adequate contingency measures are an integral part of the BCM framework which includes all key assets that supports service provisioning. In terms of BCM, assets include:

- Buildings;
- Equipment;
- Systems;
- Trust information;
- People.

Testing Preparedness; The benefits of BCM contribute towards reducing the overall disruption to service provisioning which serious events typically inflict upon a business from time to time. These benefits manifest themselves as follows:

- A means of assessing extreme risks, organisational vulnerability and threats and prioritising recovery solutions;

- Demonstrating the organisations commitment to business continuity, its stakeholders and shareholders;
- Maintaining confidence in the organisation at a time when disasters are a public concern.

Linking to Trust Risk Management; All information security risk management activities directly associated with BCM shall be conducted in accordance with Trust risk guidance. Divisions undertaking any risk assessments to articulate potential impact of disruption must evaluate these risks using recognised local risk criteria.

5 TRAINING/SUPPORT

It is mandatory that staff receive annual Information Governance training (which includes information security management) on induction and subsequently as part of a rolling programme, especially where they handle or process Person Identifying Data (PID).

Further support will be provided by IT Security in the form of security briefings, monthly guidance notes and bespoke training for both clinicians and support staff.

The training requirements of staff will be identified through a training needs analysis. Role specific education will be delivered by the service head.

6 MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT

Monitoring the effectiveness of the policy will be achieved through periodic audit with the results going to the Information Governance Group to the Finance & Performance Committee and the Board of Directors.

The IT Security Manager will perform additional auditable checks on the implementation of published security policies. Any serious risks identified will be reported to the Information Governance Group for awareness.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Patch policy compliance status	IT Security & Continuity Manager	Monthly	Cyber Security working group IG group
Number of cyber security incidents successfully managed	IT Security & Continuity Manager	Monthly	Cyber Security working group IG group
Number of known vulnerability instances	IT Security & Continuity Manager	Monthly	Cyber Security working group IG group

Number of information risk assessments completed	IT Security & Continuity Manager	Monthly	Cyber Security working group IG group
Number of penetration tests completed	IT Security & Continuity Manager	Monthly	Cyber Security working group IG group

7 DEFINITIONS

For the purposes of this document the following definitions apply:

Item	Definition
Access control	The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.
Asset owner	Individual or organisation having responsibility for specified information asset(s) and for the maintenance of appropriate security measures.
Audit trail	Data collected and potentially used to facilitate any reconstruction of events within the system.
Availability	Information is delivered to the right person, when it is needed.
Confidentiality	Data access is confined to those with specified authority to view the data.
Impact	The embarrassment, harm, financial loss, legal or other damage which could occur in consequence of a particular security breach.
Integrity	All system assets are operating correctly according to specification and in the way that the current user believes them to be operating
Security breach	Any event that has, or could have, resulted in loss or damage to NHS assets, or an action that is in breach of NHS security procedures.
Threat	An action or event that might prejudice security.

8 EQUALITY IMPACT ASSESSMENT

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are disadvantaged over others. Our objectives and responsibilities relating to equality and diversity are outlined within our equality schemes. When considering the needs and assessing the impact of a procedural document any discriminatory factors must be identified.

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Fair Treatment For All Policy (CORP/EMP 4).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (See Appendix 2).

9 ASSOCIATED TRUST PROCEDURAL DOCUMENTS

Access to Health Records Policy - CORP/REC 3
Information Systems Registration Policy - CORP/ICT 3
Equality Analysis Policy - CORP/EMP 27
Fair Treatment for All Policy – CORP/EMP 4

10 REFERENCES

All staff members are required to comply in particular with the provision of the following legislation and Department of Health guidance:

- Data Protection Act 2018
- General Data protection Regulation (GDPR) 2016/18
- Computer Misuse Act 1990
- Copyrights, Designs & Patents Act 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- The Health & Social Care Act 2012
- NHS Digital : Records Management : Code of Practice
- Mental Health Capacity Act 2005
- NHS Confidentiality Code of Practice 2003

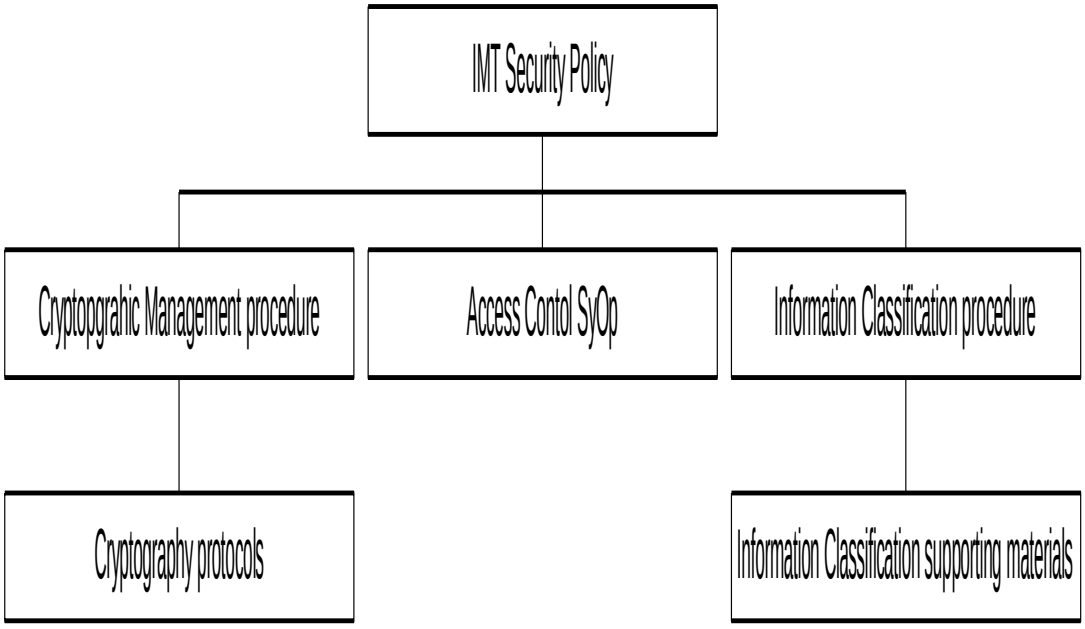
APPENDIX 1 – OVERVIEW OF IM&T SECURITY POLICY FRAMEWORK

Overview

This top-level IM&T Security policy should be considered as a key component of the organisation's overall security management framework and should be considered alongside more detailed IT security documentation.

This policy statement exists as the key document of a wider security policy framework which will include associated guidance and system operating procedures. This will ensure that all key guidance can be codified in relevant documentation rather than loaded into a single policy statement.

Figure One. Summary of IMT Security Policy framework



In the figure above the IM&T Security Policy is underpinned by specific guidance with regard to critical security domains, for example cryptographic management procedure.

By establishing the principles for guidance in the main security policy it is possible to provide staff with greater detail in the associated management procedure to ensure that relevant staff receive the codified procedures to aid service delivery.

This may also link to supporting protocols that add further detail to individual policy processes as part of Trust security management.

APPENDIX 2 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	Care Group/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
IM&T Policy – CORP/ICT 2 v.5	Chief Executives	R Smith	Existing	10 October 2017

1) Who is responsible for this policy? Name of Care Group/Directorate: IM&T

2) Describe the purpose of the service / function / policy / project/ strategy? Who is it intended to benefit? What are the intended outcomes? This policy sets the technical and organisational controls for the management of IMT security across the Trust. It defines the scope and responsibilities across services and outlines the technical requirements for the management of all aspects of IM&T security.

3) Are there any associated objectives? Legislation, targets national expectation, standards: There are a range of supporting standards defined in Appendix 1 of this policy document.

4) What factors contribute or detract from achieving intended outcomes? -

5) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief? Details: [see Equality Impact Assessment Guidance] – None.

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation] -

6) Is there any scope for new measures which would promote equality? [any actions to be taken] No.

7) Are any of the following groups adversely affected by the policy?

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box

Outcome 1 ✓	Outcome 2	Outcome 3	Outcome 4

Date for next review: February 2021

Checked by: N Hall, Head of IT Operations **Date:** June 2018